We claim:

1. A method providing security for a plurality of data records stored on a computer-readable medium within a computing system, wherein

said computer readable medium additionally stores a first data structure, starting at a first location within said computer readable medium, locating data records in said plurality thereof,

said method comprises an encryption subroutine executed as said computing system is being shut down and a decryption subroutine executed as said computing system is being initialized,

said encryption subroutine includes receiving a request to shut down said computing system, reading said first data structure from said computer readable medium, encrypting said first data structure to produce an encrypted version of said first data structure, deleting said first data structure from said computer readable medium, and storing said encrypted version of said first data structure in nonvolatile storage, starting at a second location within said nonvolatile storage, and

said decryption subroutine includes determining that electrical power has been turned on in said computing system, reading said encrypted version of said first data structure from said nonvolatile storage, decrypting said encrypted version of said first data structure to form said first data structure, and writing said data structure to said computer readable medium, starting at said first location.

2. The method of claim 1, wherein said second location is on said computer readable medium

.

3. The method of claim 2, wherein said second location is at said first location.

4. The method of claim 1, wherein said nonvolatile storage is a memory structure, separate from said computer readable medium, within said computing system.

5. The method of claim 1, wherein

encryption of said first data structure occurs within a cryptographic processor in said computing system using an encryption key,

said cryptographic processor is separate from a system processor within said computing system, and

decryption of said encrypted version of said first data structure occurs within said cryptographic processor in said computing system using a decryption key generated from data stored in secure storage accessed by said cryptographic processor.

6. The method of claim 1, wherein

a public key of said computing system is used for encryption of said first data structure, and

a private key of said computing system is used for decryption of said encrypted version of said first data structure.

7. The method of claim 1, wherein said encrypted version of said first data structure is equal in length to said first data structure.

8. The method of claim 1, wherein

said computer readable medium additionally stores a second data structure, starting at a second location within said computer readable medium, describing characteristics of said first data structure, and

said encryption subroutine additionally includes reading said second data structure to determine characteristics of said first data structure.

9. The method of claim 8, wherein

said first data structure is a file allocation table, and

said second data structure is a boot record.

10. The method of claim 8, wherein

said first data structure includes an array of file records in a master file table of a NTFS file, and

said second data structure includes metafile data in said master file table.

11. The method of claim 1, wherein

said method additionally comprises a configuration subroutine providing a user interface for setting and resetting a configuration bit, and

said encryption subroutine is executed according to a state of said configuration bit.

12. The method of claim 11, wherein

said encryption subroutine additionally includes setting a flag bit in non-volatile storage, and

said decryption subroutine is executed only when said flag bit is set.

13. A method providing security for a plurality of data records stored on a computer readable medium within a computing system, wherein

said computer medium additionally stores a first data structure starting at a first location within said removable computer readable medium, locating data records in said plurality thereof,

said method comprises an encryption subroutine executed to encrypt said first data structure and a decryption subroutine subsequently executed to decrypt an encrypted version of said first data structure,

said encryption subroutine includes reading said first data structure from said computer readable medium, encrypting said first data structure within a cryptographic processor in said computing system using an encryption key to

produce an encrypted version of said first data structure, deleting said first data structure from said computer readable medium, and storing said encrypted version of said first data structure in nonvolatile storage, starting at a second location within said nonvolatile storage, and

said decryption subroutine includes reading said encrypted version of said first data structure from said nonvolatile storage, decrypting said encrypted version of said first data structure within said cryptographic processor in said computing system using a decryption key generated from data stored in secure storage accessed by said cryptographic processor to form said first data structure, and writing said data structure to said computer readable medium, starting at said first location.

14. The method of claim 13, wherein

said encryption subroutine is executed in response to receiving a request to shut down said computing system, and

said decryption subroutine is executed in response to electrical power being turned on within said computing system.

15. The method of claim 14, wherein

said method additionally comprises a configuration subroutine providing a user interface for setting and resetting a configuration bit, and

said encryption subroutine is executed according to a state of said configuration bit.

16. The method of claim 15, wherein

said encryption subroutine additionally includes setting a flag bit in non-volatile storage, and

said decryption subroutine is executed only when said flag bit is set.

17. The method of claim 13, wherein

said method additionally comprises a cryptographic selection subroutine providing a graphical user interface,

said cryptographic selection subroutine includes displaying a choice between encryption and decryption, displaying representations of computer readable medium in said computing system, and receiving a cryptographic selection signal indicative of whether encryption or decryption is to occur and of a chosen computer readable medium,

said encryption subroutine is executed in response to receiving a cryptographic selection signal indicating encryption is to occur, with said first data structure of said chosen computer readable medium being encrypted, and

said decryption subroutine is executed in response to receiving a cryptographic selection signal indicating decryption is to occur, and with said encrypted version of said first data structure of said chosen computer readable medium being decrypted.

18. The method of claim 17, wherein said encrypted version of said first data structure is stored in nonvolatile storage on said chosen computer readable medium.

19. A computing system providing secure storage of a plurality of data records comprising:

a first computer readable medium storing said plurality of data records and a first data structure providing locations and sequences for accessing data within said data records;

a first drive unit recording data on said first computer readable medium and reading data from said computer readable medium;

nonvolatile storage;

a cryptographic processor, wherein said cryptographic processor is

programmed to execute an internal encryption routine to encrypt a data structure, forming an encrypted version of said data structure using an encryption key, and to execute subsequently an internal decryption routine, decrypting said encrypted version of said data structure, using a decryption key;

secure storage. accessed by said cryptographic processor, holding data used within said cryptographic processor to derive said decryption key;

a microprocessor, separate from said cryptographic processor, wherein said microprocessor is programmed to execute a data structure encryption routine to encrypt said first data structure and to execute subsequently a data structure decryption routine to decrypt an encrypted version of said first data structure, wherein said data structure encryption routine includes causing said cryptographic processor to read said first data structure from said computer readable medium, to execute said internal encryption routine, encrypting said data structure to form said encrypted version of said first data structure, and to write said encrypted version of said first data structure to nonvolatile storage, wherein said first data structure is additionally deleted from said first computer readable medium during execution of said data structure encryption subroutine, and wherein said data structure decryption subroutine includes causing said cryptographic processor to read said encrypted version of said first data structure from nonvolatile storage, to decrypt said encrypted version of said first data structure, forming said first data structure, and to write said first data structure to said computer readable medium, starting at said first location.

20. The computing system of claim 19, wherein

said first drive unit is a hard drive,

said data structure encryption subroutine is executed in response to receiving a request to shut down said computing system, and

said data structure decryption subroutine is executed in response to electrical power being turned on within said computing system.

21. The computing system of claim 20, wherein

said microprocessor is additionally programmed to execute a configuration subroutine providing a user interface for setting and resetting a configuration bit, and

said encryption subroutine is executed according to a state of said configuration bit.

22. The computing system of claim 21, wherein

said encryption subroutine additionally includes setting a flag bit in non-volatile storage, and

said decryption subroutine is executed only when said flag bit is set.

23. The computing system of claim 19, wherein

said computer readable medium is removable,

said method additionally comprises a cryptographic selection subroutine providing a graphical user interface,

said cryptographic selection subroutine includes displaying a choice between encryption and decryption, displaying representations of computer readable medium in said computing system, and receiving a cryptographic selection signal indicative of whether encryption or decryption is to occur and of a chosen computer readable medium,

said encryption subroutine is executed in response to receiving a cryptographic selection signal indicating encryption is to occur, with said first data structure of said chosen computer readable medium being encrypted, and

said decryption subroutine is executed in response to receiving a cryptographic selection signal indicating decryption is to occur, and with said encrypted version of said first data structure of said chosen computer readable medium being decrypted.

24. The computing system of claim 23, wherein said encrypted version of said

first data structure is stored in nonvolatile storage on said chosen computer readable medium.

25. The computing system of claim 19, wherein

said computer readable medium additionally stores a second data structure, starting at a second location within said computer readable medium, describing characteristics of said first data structure, and

said data structure encryption subroutine additionally includes reading said second data structure to determine characteristics of said first data structure.